Software Engineering Institute
Carnegie Mellon University

Emerging Technology Domains Risk Survey

Christopher King
Jonathan Chu
Andrew Mellinger

April 2015

TECHNICAL NOTE
CMU/SEI-2015-TN-003

CERT Division

http://www.sei.cmu.edu

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

This report was prepared for the
SEI Administrative Agent
AFLCMC/PZM
20 Schilling Circle, Bldg 1305, 3rd floor
Hanscom AFB, MA 01731-2125

DM-0002074

Table of Contents

List of Figures

List of Tables

Abstract

In today's increasingly interconnected world, the information security community must be prepared to address emerging vulnerabilities that may arise from new technology domains. Understanding trends and emerging technologies can help information security professionals, leaders of organizations, and others interested in information security to anticipate and prepare for such vulnerabilities. This report, originally prepared in 2014 for the Department of Homeland Security United States Computer Emergency Readiness Team (US-CERT), provides a snapshot in time of the current understanding of future technologies. Each year, this report will be updated to include new estimates of adoption timelines, new technologies, and adjustments to the potential security impact of each domain. This report will also help US-CERT to make an informed decision about the best areas to focus resources for identifying new vulnerabilities, promoting good security practices, and increasing understanding of systemic vulnerability risk.

Executive Summary

> *"The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it."*
>
> *–Mark Weiser*[1]

Mark Weiser first coined the term "ubiquitous computing," describing it as an "invisible, everywhere computing that does not live on a personal device of any sort, but is in the woodwork everywhere."[2] With advancements in miniaturization and in the economies of scale for systems-on-a-chip, Weiser's vision is finally becoming a reality.

Weiser's vision of the future also included the difficult challenge of securing the near-infinite amounts of data generated, processed, and stored by ubiquitous devices (or in today's parlance, the "Internet of Things"). This increasing prevalence of new devices—and the extent to which Americans have come to rely on these devices in daily life—presents new challenges for the vulnerability coordination community as well. Can the Common Vulnerability Enumeration (CVE) methodology support this myriad of devices? Can the Common Vulnerability Scoring System (CVSS) provide effective and meaningful vulnerability information as increasingly complex and interrelated vulnerabilities surface?

The Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) "strives for a safer, stronger Internet for all Americans by responding to major incidents, analyzing threats, and exchanging critical cybersecurity information with trusted partners around the world." To carry out its mission, US-CERT must be proactive, focusing on future threats and vulnerabilities while attempting to ignore the fear, uncertainty, and doubt that is often spread by the cybersecurity community and media.

To support the US-CERT mission of proactivity, the CERT Coordination Center (CERT/CC) located at Carnegie Mellon University's Software Engineering Institute was tasked with studying emerging systemic vulnerabilities, defined as exposures or weaknesses in a system that arise due to complex or unexpected interactions between subcomponents. The CERT/CC researched the emerging technology trends through 2024 to assess the technology domains that will become successful and transformative, as well as the potential cybersecurity impact of each domain. This report is intended to provide a brief background of each emerging technology domain, the potential vulnerabilities the domain possesses, and the impact of compromise or failure within the domain. In addition, this report identifies the domains that should be prioritized for further study based on a number of factors.

Five domains must be considered high-priority for corporate outreach and analysis in 2014:

- **Vehicle Autonomy**: for example, self-driving cars and trucks

[1] http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html

[2] http://www.ubiq.com/hypertext/weiser/UbiHome.html

- **Smart Sensors**: such as networked sensors that are considered to be part of the "Internet of Things"
- **Smart Appliances**: everyday appliances, such as washing machines and dryers that are IP-enabled and controllable via the network
- **Networked Telematics**: dashboard vehicular information and entertainment systems
- **Smart Medical Devices**: such as networked, compute-enabled medical devices

This list does not imply that each domain will require detailed analysis. Every domain is nuanced, and some domains may require further study earlier in the development lifecycle of the domain than others. Different approaches to improving security should be taken depending on the specific nature of each domain. In some cases, outreach is the best approach for improving the security of a technology; in other cases, technical vulnerability discovery may be the best way to provide better information to the government and public. This report includes a specific approach recommended by the CERT/CC for improving security in each domain.

Each year this report will be updated to include new domains, reassess the cybersecurity impact of each domain, and adjust the adoption timeline as needed. Further work in identifying systemic vulnerabilities will rely upon the findings in this first report.

1 Introduction

As the technological world becomes increasingly interconnected, information security vulnerabilities become more complex. Interactions between hardware and software subcomponents can magnify the impact of a vulnerability. The shift from single computers to a cloud environment that supports a myriad of devices and sensors introduces even more complexity.

The information security community must be prepared to address emerging systemic vulnerabilities—exposures or weaknesses in a system that are introduced due to complex or unexpected interactions between subcomponents. To help identify these vulnerabilities, the CERT Coordination Center (CERT/CC) located at Carnegie Mellon University's Software Engineering Institute developed this report that breaks down the major technology trends expected over the next 10 years. This report provides the background for further analysis work by the CERT/CC and will aid the Department of Homeland Security United States Computer Emergency Readiness Team (US-CERT) in its work towards vulnerability triage, outreach, and analysis.

The goal of this report is to provide a snapshot in time of the current understanding of future technologies. Each year, this report will be updated to include new estimates of adoption timelines, new technologies, and adjustments to the potential security impact of each domain. This report will also form the basis for making an informed decision about the best areas to focus resources when US-CERT would like to identify new vulnerabilities, promote good security practices, and increase understanding of systemic vulnerability risk.

Report Format

This report presents information on 13 emerging domains[3] and aims to provide the reader with

- an understanding of the major emerging technology domains
- the expected timeline for major worldwide adoption
- the potential impact on information security the domain may have
- supporting standards and underlying technologies used by these domains
- likelihood of the domain becoming a success
- examples of exploitation in the domain or similar domains

The format of this report allows readers to quickly jump to a section and familiarize themselves with a domain. Each domain section contains the following subsections:

1. **Introduction** serves as a background on the application domain.
2. **Recommendation** includes the CERT/CC's recommendation for US-CERT on addressing this domain.
3. **Time Frame** addresses the time in which broad adoption is likely.

[3] In this report, the term "domain" is used to describe a particular field of technology.

4. **Impact** provides a discussion of the potential impact of security vulnerabilities in the domain.
5. **Likelihood of Domain Success** examines factors indicating whether a technology will achieve adoption.
6. **Triage Table** describes the measures upon which the CERT/CC based its recommendations and how each domain was triaged for importance.
7. **Exploitation Examples** details concepts or existing research demonstrating exploits of this domain.
8. **References** shows the external data used to support the recommendations and analysis.

2 Methodology

A measured approach to analysis is required when undertaking the difficult task of reviewing all new and emerging technology domains, their likelihood of success, and any potential vulnerabilities. The CERT/CC relied on Gartner's long-term assessment of technologies to form its initial list of domains. Gartner subscribers can access a list of "hype cycles" that describe each technology, its current maturity in the market, and when Gartner believes it will reach mainstream adoption in its industry [Fenn 2013]. This list tracks over 1,700 different technologies from inception to full adoption. From this list, the CERT/CC team identified domains likely to have an impact on global information security. Domains that were not included were either already widely deployed (e.g., mobile, cloud computing, supervisory control and data acquisition [SCADA]) or simply not applicable. The team "triaged" each identified domain by assessing several characteristics important to security, including remote access potential, processing power, danger to human lives, and digital consequences (see Table 1). The team then assessed each domain individually to determine its likelihood of success, potential impact if compromised, exploitation examples, and adoption timeline.

Table 1: Domain Triage: Characteristics and Questions

Characteristic/Question	Explanation
Market Segment	This field describes the market segment group that this domain is targeting. Available options: Niche, Industry, Government, Consumer, Comprehensive (i.e., any/all), and Other
Potential Market Segment Size	What is the potential size of the market, in dollars? Available options: <$1B, $1B-$25B, $25B-$50B, >$50B
Projected Adopters (percentage of market segment)	What is the projected number of users of this technology? This is represented as a percentage of the market segment. Available options: <25%, 25-50%, 50-75%, >75%
Current Market Penetration	Approximately what portion of the market population has adopted the technology? This is represented as a percentage. Available options: <25%, 25-50%, 50-75%, >75%
Predicted Adoption Timeline	Gartner's predicted technology adoption timeline. Represented in both number of years and target dates.
Does the technology have direct physical impact on the world?	In order to evaluate risk, we wanted to determine the direct impact on the physical world. The ability to directly influence and manipulate the physical world affects the potential for harm when compromised. Available options: Yes, No
Can it cause direct property damage?	If the technology is able to directly manipulate the physical world, can it directly cause property damage? Available options: Yes, No
Can it cause direct human harm?	If the technology is able to directly manipulate the physical world, can it cause harm to humans? Available options: Yes, No
What is the scale of human harm?	If the technology is able to harm human beings, how many humans can it harm? Available options: none, single person, 1-10 people, > 10 people

Characteristic/Question	Explanation
Digital consequence	Are there implications for confidentiality, integrity, or availability if this technology is compromised? Available options: Yes [implication], No
Is this domain intended to be remotely accessible?	This question evaluates the remote exploitability of a technology. Available options: Yes, No
Is this domain intended to be Internet accessible?	If this domain is remotely accessible, is the intended deployment for the Internet? Global availability has broad implications for withstanding attempts to exploit. Available options: Yes, No
Is this domain intended to be accessible to the local network?	If this domain is remotely accessible, is it available via local networks? Local network availability means it is available as a lateral movement within a network. Available options: Yes, No
Does this domain connect or bridge multiple networks?	This question considers the potential for lateral movement between networks. A device that bridges networks has multiple fronts to defend. Available options: Yes, No
NOTES:	Any additional comments from the CERT/CC evaluation team.

3 Broadband-Connected Televisions

3.1 Introduction

In an effort to improve sales, manufacturers of televisions have increasingly added smartphone-like functionality to their models. These broadband-connected televisions, which are sometimes marketed as "smart TVs," usually contain an Ethernet port and/or a Wi-Fi chipset for connectivity. The TV contains limited processing power, enough to run a separate application environment that users can launch with their TV remote or smartphone application. The applications vary in complexity but usually provide Internet video services and web search functionality.

3.2 Recommendation

Although broadband-connected televisions are an area of concern, the lack of persistent storage and limited damage potential make this domain less of a priority than others. The CERT/CC recommends making this domain a focus in 2015, while dedicating limited resources in 2014 to encouraging smart TV manufacturers to produce secure products.

3.3 Time Frame

From the CERT/CC perspective, this technology should be prioritized now: in 2013, 22% of TVs sold were broadband-enabled [Chen 2014].

3.4 Impact

Adding an always-on or often-on device to a household—when that device is also mostly ubiquitous (there are 115 million homes with TVs [Nielsen 2013])—can pose risks for the home user. However, because these devices are not traditional storage devices with large amounts of disk space or memory, damage can be limited. The concern is that smart TVs are not seen as traditional computing devices that need patch cycles, software firewalls, and good security practices. To most consumers a smart TV is simply another TV, but it has the potential for becoming a foothold into the home network. Privacy is also a concern: attackers can find out what a person watches, and attackers may be able to spy on people whose TVs have web cams [Leyden 2012].

3.5 Likelihood of Domain Success

This domain is extremely likely to be successful. Consumers will increasingly replace their old TVs with smart TVs. Furthermore, it is likely that existing embedded operating systems (OS) such as Google's Android or Apple's iOS will be integrated closely in the future. Consumers have little patience for one-off, poorly designed application interfaces in their televisions. With the support of a major software company and integration of a familiar OS, adoption of broadband-enabled TVs will probably rise [Levy 2014].

3.6 Exploitation Examples

In August 2013, security researchers were able to hack into a particular model of Samsung smart TV. The researchers discovered that that these devices have one user with administrative privileges. Once the device is compromised, the attacker has full access to all of the functions of the device. In this case, the researchers were able to access the built-in camera and use it to spy on people [Fink 2013].

3.7 Triage Table

Table 2: Domain Triage for Broadband-Connected Televisions

Characteristic/Question	Findings
Market Segment (Niche, Industry, Government, Consumer, Comprehensive, Other)	Consumer
Potential Market Segment Size (<$1B, $1B-$25B, $25B-$50B, >$50B)	$25B-$50B
Projected Adopters (Percentage of market segment)	>75%
Current Market Penetration (Percentage)	<25%
Predicted Adoption Timeline (Years)	5 to 10 years
Does the technology have direct physical impact on the world? (Yes, No)	No
Can it cause direct property damage? (Yes, No)	No
Can it cause direct human harm? (Yes, No)	No
What is the scale of human harm? (none, single person, 1-10 people, > 10 people)	None
Digital consequence (Yes, No)	Yes
Is this domain intended to be remotely accessible? (Yes, No)	Yes
Is this domain intended to be Internet accessible? (Yes, No)	Yes
Is this domain intended to be accessible to the local network? (Yes, No)	Yes
Does this domain connect or bridge multiple networks? (Yes, No)	No

4 Enterprise 3D Printing (Additive Manufacturing)

4.1 Introduction

3D printing is an "additive technique" used to create three-dimensional objects by applying physical materials iteratively via an automated system. The term "printing" refers to the way an inkjet printer creates an image: by iteratively depositing ink over a sheet of paper. In 3D printing, materials such as plastics, fibers, or even metallic compounds can be used. The term "additive manufacturing" is becoming more commonplace.

3D printing has two general purposes in the enterprise: to generate prototypes in research, development, and product design, and to create actual products to sell to consumers. 3D printers constantly evolve to use more complex and durable materials, and their potential uses are increasing [Burns 2014].

4.2 Recommendation

The CERT/CC recommends further review of this domain in 2015. There is currently little evidence to suggest information security problems with 3D printing, but this situation may change as 3D printing enables consumers to print circuit boards and other electronic hardware.

4.3 Time Frame

3D printing has the potential to disrupt current manufacturing processes but will not be used by consumers at home in the near future. Adoption is expected to be small scale and used primarily as a prototyping device for the next few years [Dignan 2014]. Today, a variety of 3D printers are already available, and rapid growth and decreased cost are expected in the near future [Burns 2013; Franco 2014].

4.4 Impact

Additive manufacturing is not an area of explicit security concern. These devices contain Ethernet or Wi-Fi connectivity, a programmable logic controller, and various servomechanisms to control the heating units and distribution nozzles. While a security compromise of this device could result in damage to the device or the surrounding area (due to the heated material produced), these risks are not fundamentally different from those posed by existing industrial machinery.

One area that may prove to be a challenge to the information security community is the ability to custom-print keys (affecting physical security) or programmable logic boards or controllers. Cheap microcontroller/board development and open source designs allow for essentially unlimited production of sensors, micro PCs, and specialized equipment by a single individual. This democratization of hardware will have effects on the existing ecosystem of devices and systems that is difficult to predict.

4.5 Likelihood of Domain Success

Research and development and prototyping groups already make significant use of 3D printers and will continue to do so. In the near term, custom parts can be produced at various tooling companies that will become the first adopters of 3D printing. In the long term, the 3D printer may become just another tool like an auto-lathe or robotic assembly station.

4.6 Exploitation Examples

3D printers allow access to shapes and materials that were previously difficult to acquire in a covert fashion; 3D printers have been used to print restricted-use items such as secure handcuff keys and handgun parts [Greenberg 2012; Hsu 2013a; Hsu 2013b].

3D printers can also be compromised directly leading to other challenges [Xiao 2013; Titlow 2013]. As with a variety of automated manufacturing machines, the 3D printer must be configured with instructions that tell the printer what materials to deposit and where to place them. These instructions represent valuable intellectual property that can be stolen or even modified in place to produce "defective" items. In this way, 3D printing exposes all supply chain vulnerabilities and impacts, from manufacturing problems to impacts to customers when defects are not easily detected.

4.7 Triage Table

Table 3: Domain Triage for 3D Printing

Characteristic/Question	Findings
Market Segment (Niche, Industry, Government, Consumer, Comprehensive, Other)	Comprehensive
Potential Market Segment Size (<$1B, $1B-$25B, $25B-$50B, >$50B)	$1B-$25B
Projected Adopters (Percentage of market segment)	<25%
Current Market Penetration (Percentage)	<25%
Predicted Adoption Timeline (Years)	2 to 5 years
Does the technology have direct physical impact on the world? (Yes, No)	Yes
Can it cause direct property damage? (Yes, No)	Yes
Can it cause direct human harm? (Yes, No)	No
What is the scale of human harm? (none, single person, 1-10 people, > 10 people)	None
Digital consequence (Yes, No)	Yes
Is this domain intended to be remotely accessible? (Yes, No)	Yes
Is this domain intended to be Internet accessible? (Yes, No)	No
Is this domain intended to be accessible to the local network? (Yes, No)	Yes
Does this domain connect or bridge multiple networks? (Yes, No)	No

5 Home Area Network

5.1 Introduction

A Home Area Network (HAN), an outgrowth of the traditional Local Area Network (LAN), is simply a network that connects PCs, smartphones, tablets, smart sensors, and other devices together into one network that shares a common Internet connection. In contrast to traditional LANs, HANs bring together the external Internet, local Wi-Fi/Ethernet network, Bluetooth, and other communications technologies (such as mesh networking). See Appendix A for more details on the different types of network classifications.

5.2 Recommendation

The CERT/CC recommends studying the Home Area Network domain within the context of other domains as they are analyzed. This domain has been studied in the past, but implications for home users (including concerns related to ISP-provided equipment, smart appliances, wireless-enabled cars, energy monitoring, and other sensors) have not been fully considered.

5.3 Time Frame

The CERT/CC considers HANs a nascent area of development. Most homes already have some sort of HAN, usually just a router, connected PCs, smartphones, and tablets. As technology progresses, this list will likely change to include smart appliances and other devices that will use the shared Internet connection to communicate with vendors or other services.

5.4 Impact

The best protection most home users have is an ISP-provided router that is set by default to block all incoming connections on the WAN port and has default WPA2 encryption on the wireless side. As more devices are added to the home network, a secure router will likely remain the best type of protection for the home user. However, network-bridging devices, such as those with both Bluetooth and Wi-Fi services or mesh-networked sensors that connect via their own wireless protocol and to Wi-Fi, can open the home network to attacks.

5.5 Likelihood of Domain Success

This domain is extremely likely to be successful. There are already nascent HANs deployed throughout the world, and with the proliferation of Internet-enabled devices that depend on a home wireless or wired connection, HANs will likely become the underlying support infrastructure for those devices. Though it is possible that broadband cellular connections will become the infrastructure of choice, lower speeds and reliability as well as the relatively high cost of service currently makes this an untenable choice for consumers.

5.6 Triage Table

Table 4: Domain Triage for the Home Area Networks

Characteristic/Question	Findings
Market Segment (Niche, Industry, Government, Consumer, Comprehensive, Other)	Consumer
Potential Market Segment Size (<$1B, $1B-$25B, $25B-$50B, >$50B)	$25B-$50B
Projected Adopters (Percentage of market segment)	>75%
Current Market Penetration (Percentage)	<25%
Predicted Adoption Timeline (Years)	5 to 10 years
Does the technology have direct physical impact on the world? (Yes, No)	No
Can it cause direct property damage? (Yes, No)	No
Can it cause direct human harm? (Yes, No)	No
What is the scale of human harm? (none, single person, 1-10 people, > 10 people)	None
Digital consequence (Yes, No)	Yes
Is this domain intended to be remotely accessible? (Yes, No)	Yes
Is this domain intended to be Internet accessible? (Yes, No)	Yes
Is this domain intended to be accessible to the local network? (Yes, No)	Yes
Does this domain connect or bridge multiple networks? (Yes, No)	No

5.7 Exploitation Examples

This domain is mainly an infrastructure component that provides access to other devices. Consumer premise equipment (CPE) has been exploited due to poor configuration choices by the manufacturer or ISP. A portion of CPE devices contain open DNS resolvers that can be exploited in various ways; the most concerning attacks are record injection and cache poisoning [Schomp 2014].

6 Networked Telematics

6.1 Introduction

"Telematics" refers to the electronics, communication, and display technology associated with vehicular dashboard systems. Telematics encompasses all functions of the vehicle electronics that are designed to be accessible to users. The dashboard, controls, and navigation system are parts of the telematics system. Many vehicle manufacturers have recently added cellular connectivity to their vehicles to provide richer, more interactive services to the consumer. Developers of smartphone operating systems have also begun to integrate their products more closely with telematics systems.

6.2 Recommendation

The CERT/CC recommends prioritizing this domain for outreach in 2014. The upcoming mass deployment of this domain will increase the risk of new vulnerabilities, especially those of a systemic nature. The emerging smartphone-telematics integration technologies (Apple CarPlay, Google Open Automotive Alliance, Blackberry QNX) are of particular concern.

6.3 Time Frame

Telematics systems, in varying levels of complexity, are deployed on practically every vehicle in the world. In the past, only a few vehicles had access to a cellular Internet connection, and only at 3G speeds. Some vehicles already have LTE connections, and many manufacturers plan to add them to future models [Cheng 2013, George 2014].

6.4 Impact

Telematics should be considered a high-risk domain for systemic vulnerabilities. A telematics system is very tightly integrated with other systems in a vehicle and provides a number of functions for the user. The recent additions of wireless connectivity such as Bluetooth, Wi-Fi, and LTE increase the risk of compromise. An Internet-connected vehicle is vulnerable to a wide range of attacks, both from determined attackers and from traditional threats such as malicious code and phishing.

6.5 Likelihood of Domain Success

This sector has a very high likelihood of success. Telematics systems are already deployed on most vehicles worldwide, and the major car manufacturers have announced that some 2015 models will include LTE connections [Cheng 2013, George 2014].

6.6 Triage Table

Table 5: Domain Triage for Networked Telematics

Characteristic/Question	Findings
Market Segment (Niche, Industry, Government, Consumer, Comprehensive, Other)	Comprehensive
Potential Market Segment Size (<$1B, $1B-$25B, $25B-$50B, >$50B)	$25B-$50B
Projected Adopters (Percentage of market segment)	>75%
Current Market Penetration (Percentage)	<25%
Predicted Adoption Timeline (Years)	2 to 5 years
Does the technology have direct physical impact on the world? (Yes, No)	No
Can it cause direct property damage? (Yes, No)	No
Can it cause direct human harm? (Yes, No)	No
What is the scale of human harm? (none, single person, 1-10 people, > 10 people)	None
Digital consequence (Yes, No)	Yes
Is this domain intended to be remotely accessible? (Yes, No)	Yes
Is this domain intended to be Internet accessible? (Yes, No)	Yes
Is this domain intended to be accessible to the local network? (Yes, No)	Yes
Does this domain connect or bridge multiple networks? (Yes, No)	Yes

6.7 Exploitation Examples

Academic researchers have looked deeply into the varied attack surfaces within vehicular systems, focusing on telematics in particular. This research has shown that it is possible to compromise a vehicle remotely via Bluetooth, malware-infected CDs, and through USB connection [Checkoway 2011].

7 Phone-as-a-Token

7.1 Introduction

Phone-as-a-token is an authentication method by which a smartphone provides the security token in the authentication process either as an out-of-band (OOB) device (e.g., using text messaging) or by generating a one-time-password (OTP) for an application.

It is important to note that while both authentication methods provide two-factor authentication, they do not provide equivalent security protection; of the two methods, OTPs offer greater security.

7.2 Recommendation

The CERT/CC recommends limited involvement in this domain. There is significant deployment in this area already, and any outreach efforts may be of limited utility. The CERT/CC recommends investigating the size of the market, identifying the major standards bodies relevant to this domain, and beginning outreach to those organizations in 2014.

7.3 Time Frame

A variety of applications use two-factor authentication with smartphones. Many online games use smartphones in the OTP role to generate additional security tokens. The online game World of Warcraft has been using phone-as-a-token since 2008 [Danchev 2008].

7.4 Impact

Considering the significant existing adoption and the central role this technology plays in the authentication process, phone-as-a-token will become a significant part of the attack surface.

In the case of out-of-band (OOB) authentication, the overall authentication system relies on a channel to a device that is independent from the authenticating system. For example, imagine that a user is trying to authenticate to a site from a desktop PC, and the site requires the user to authenticate using a PIN over short-message service (SMS), or text messaging. Normally the PIN is sent via a channel separate from the initial connection (the web browser); in this case, the separate channel is the cellular network to the phone. Now imagine that the user is trying to authenticate on the same machine to which the OOB message will be sent. For example, what if the user is authenticating via a browser on the phone that is also the recipient of the text message? What if the text message is routed through a service to the same desktop? In both cases, malware on one device could have access to both channels and subvert the value of the out-of-band authentication.

OTP applications on a phone (such as Google Authenticator) provide one-time passwords that expire after a brief time period and are not sent through any communication medium to the authenticating system. Despite the potential flaws in phone-as-a-token, the OTP method of authentication is likely safer than single-password and OOB methods of authentication.

7.5 Likelihood of Domain Success

Phone-as-a-token authentication methods may have significant positive security impacts because the technology is ubiquitous and easy to use. Having a readily available source of multi-factor authentication without the need to invest in custom hardware will encourage businesses to use the technology. Additionally, smartphones are easily updated to allow for regular and timely security patching.

This technology is already widely deployed as part of anti-fraud efforts. One example is Google Authenticator, an OTP application for accessing Google services; Apple provides a similar application for accessing its services. Many banks utilize OOB passwords to reduce fraud.

7.6 Triage Table

Table 6: Domain Triage for Phone-as-a-Token

Characteristic/Question	Findings
Market Segment (Niche, Industry, Government, Consumer, Comprehensive, Other)	Consumer
Potential Market Segment Size (<$1B, $1B-$25B, $25B-$50B, >$50B)	$1B-$25B
Projected Adopters (Percentage of market segment)	25-50%
Current Market Penetration (Percentage)	<25%
Predicted Adoption Timeline (Years)	2 to 5 years
Does the technology have direct physical impact on the world? (Yes, No)	No
Can it cause direct property damage? (Yes, No)	No
Can it cause direct human harm? (Yes, No)	No
What is the scale of human harm? (none, single person, 1-10 people, > 10 people)	None
Digital consequence (Yes, No)	Yes
Is this domain intended to be remotely accessible? (Yes, No)	No
Is this domain intended to be Internet accessible? (Yes, No)	No
Is this domain intended to be accessible to the local network? (Yes, No)	No
Does this domain connect or bridge multiple networks? (Yes, No)	No

7.7 Exploitation Examples

In January 2014, malware on a desktop PC captured both the password and token of a World of Warcraft account [Constantin 2014]. A more common example is malware that attempts to convince the user to download a malicious application that acts as an SMS forwarder in order to capture OOB passwords [Crosman 2013].

8 Quantified Self

8.1 Introduction

Quantified self is a set of technologies such as wearable devices that monitor a user and collect various analytics. The general use case is for health and fitness—for example, tracking the number of steps taken, level of activity, heart rate, and so on.

Quantified self devices are not medical devices (they do not apply treatment, drugs, etc.). While they do monitor user behaviors and some health statistics, they are not considered medical sensors and are not regulated as such.

8.2 Recommendation

The CERT/CC does not recommend analysis of this domain at this time. While this technology is vulnerable to criminal activity and other exploitation, quantified self devices do not provide novel systemic vulnerabilities.

8.3 Time Frame

There are numerous quantified self devices and applications available for use now, and the market is growing in popularity (3.3 million fitness trackers were sold in 2013). The FitBit, Moves App, and Withings Scale are some few of the quantified self devices and applications that are currently available [Danova 2014].

8.4 Impact

Though quantified self devices are not considered medical devices or medical sensors, they store and collect the same types of information these devices use, such as PII. Because these devices have access to a wide variety of data and are not subject to the same regulation as medical devices, leaks of user information have occurred [Rao 2011].

As with any technology that collects or stores PII and other personal behavior information, quantified self devices can be used to target an individual in scams, gain an individual's trust, or even blackmail someone.

8.5 Likelihood of Domain Success

Fitness tracking wristbands are a $2.5 billion industry, and quantified self startups are beginning to be purchased by established firms [Etherington 2014]. It is likely that this movement to "track everything" will continue to accelerate, especially as consumers and medical professionals begin to see benefits in personalized health data.

8.6 Triage Table

Table 7: Domain Triage for Quantified Self

Characteristic/Question	Findings
Market Segment (Niche, Industry, Government, Consumer, Comprehensive, Other)	Consumer
Potential Market Segment Size (<$1B, $1B-$25B, $25B-$50B, >$50B)	$1B-$25B
Projected Adopters (Percentage of market segment)	>75%
Current Market Penetration (Percentage)	<25%
Predicted Adoption Timeline (Years)	2 to 5 years
Does the technology have direct physical impact on the world? (Yes, No)	No
Can it cause direct property damage? (Yes, No)	No
Can it cause direct human harm? (Yes, No)	No
What is the scale of human harm? (none, single person, 1-10 people, > 10 people)	None
Digital consequence (Yes, No)	Yes
Is this domain intended to be remotely accessible? (Yes, No)	No
Is this domain intended to be Internet accessible? (Yes, No)	No
Is this domain intended to be accessible to the local network? (Yes, No)	Yes
Does this domain connect or bridge multiple networks? (Yes, No)	Yes

8.7 Exploitation Examples

At this time, the CERT/CC is not aware of any exploitation attempts on this domain.

9 Smart Appliances

9.1 Introduction

Smart appliances are Internet-connected forms of traditional consumer goods such as washing machines, dryers, refrigerators, coffee makers, and other machines. The low cost of wireless chipsets and processing power has enabled manufacturers to equip their appliances with basic digital features. These features include passive sensing and reporting, such as informing the user when the wash cycle has completed, and active sensing, such as allowing control of refrigerator temperature with a smartphone.

9.2 Recommendation

The smart appliance domain is still an emerging market that will not reach fruition for some time. The CERT/CC recommends reviewing this domain in 2015 to validate the progress of the technology. The market for smart appliances is currently rather small but is expected to grow in coming years. Growth within the smart appliance domain may increase more rapidly if costs drop or if an established technology company (such as Google or Apple) gets involved.

9.3 Time Frame

Because most smart appliances currently on the market are available only in high-end equipment lineups from manufacturers, market penetration in this domain is relatively low [ABI Research 2013]. Another barrier to adoption is that each manufacturer has developed its own method of communication, and pairing two smart appliances from differing manufacturers is currently impossible [Wolff-Mann 2013].

9.4 Impact

The introduction of additional devices with always-on capability can pose risks for the home user. However, because these devices are not traditional storage devices with large amounts of disk space or memory, damage can be limited. Processing power and user interfaces in these devices are similar to a smartphone but have limited applications and options. The concern is that smart appliances are not seen as traditional computing devices that need patch cycles, software firewalls, and good security practices. There is more risk if the appliance can be controlled remotely, especially if it is possible to circumvent any built-in safety controls. Overloading the protective circuits in an oven may cause a fire, and forcing a dishwasher to run water may cause damaging flooding. Danger to humans is possible as well, such as causing food to spoil in the refrigerator or overheating the water heater to scald someone in the shower.

9.5 Likelihood of Domain Success

There is a medium likelihood of success of this sector. Currently the addition of digital features is not providing clear value to the consumer. Furthermore, because consumers usually have appliances for several years, the technology may advance faster than consumers can adopt it.

9.6 Triage Table

Table 8: Domain Triage for Smart Appliances

Characteristic/Question	Findings
Market Segment (Niche, Industry, Government, Consumer, Comprehensive, Other)	Consumer
Potential Market Segment Size (<$1B, $1B-$25B, $25B-$50B, >$50B)	$25B-$50B
Projected Adopters (Percentage of market segment)	>75%
Current Market Penetration (Percentage)	<25%
Predicted Adoption Timeline (Years)	5 to 10 years
Does the technology have direct physical impact on the world? (Yes, No)	Yes
Can it cause direct property damage? (Yes, No)	Yes
Can it cause direct human harm? (Yes, No)	Yes
What is the scale of human harm? (none, single person, 1-10 people, > 10 people)	Single person
Digital consequence (Yes, No)	Yes
Is this domain intended to be remotely accessible? (Yes, No)	Yes
Is this domain intended to be Internet accessible? (Yes, No)	Yes
Is this domain intended to be accessible to the local network? (Yes, No)	Yes
Does this domain connect or bridge multiple networks? (Yes, No)	No

9.7 Exploitation Examples

There have been no accurate reports of smart appliances being compromised. Recent claims that smart refrigerators were compromised and used as part of a spam botnet turned out to be false [Rodriguez 2014, Thomas 2014]. However, recent developments in malicious code indicate increased interest in smart appliances [Hayashi 2013].

10 Smart Medical Devices

10.1 Introduction

A smart medical device is a biomechanical machine that interfaces with the human body in an inpatient or outpatient context. Recent advances in medical device development have moved the industry toward more connected devices, partly due to the benefits that the data from such devices can provide to central hospital systems. While caregivers see the trend toward smart medical devices as positive, security concerns increase as more devices are connected to the hospital network. Many of the devices in this field have little to no security, and the increased scrutiny required by the Food and Drug Administration (FDA) makes the patch cycle extremely long.

10.2 Recommendation

Due to the impact of smart medical devices on human lives, the CERT/CC recommends prioritizing outreach to this domain in 2014. The regulatory structure of this domain suggests that the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) or the FDA will be the primary champion of good security practices.

10.3 Time Frame

Smart medical device technology, part of the $68B medical device market, is already deployed in many hospitals and clinics worldwide. Though smart medical devices are not yet ubiquitous, many of the new devices hospitals purchase are network-enabled and have some form of processing power and storage. [Zhong 2012]

10.4 Impact

As more devices are connected to hospital and clinic networks, patient data and information will be increasingly vulnerable. Even more concerning is the risk of remote compromise of a device directly connected to a patient. An attacker could theoretically increase or decrease dosages, send electrical signals to a patient, or disable vital sign monitoring.

10.5 Likelihood of Domain Success

This sector has a very high likelihood of success. Many manufacturers have released connected medical devices, and hospitals and clinics are purchasing more of these devices as they upgrade their equipment.

10.6 Triage Table

Table 9: Domain Triage for Smart Medical Devices

Characteristic/Question	Findings
Market Segment (Niche, Industry, Government, Consumer, Comprehensive, Other)	Industry
Potential Market Segment Size (<$1B, $1B-$25B, $25B-$50B, >$50B)	>$50B
Projected Adopters (Percentage of market segment)	50-75%
Current Market Penetration (Percentage)	<25%
Predicted Adoption Timeline (Years)	5 to 10 years
Does the technology have direct physical impact on the world? (Yes, No)	No
Can it cause direct property damage? (Yes, No)	No
Can it cause direct human harm? (Yes, No)	Yes
What is the scale of human harm? (none, single person, 1-10 people, > 10 people)	Single person
Digital consequence (Yes, No)	Yes
Is this domain intended to be remotely accessible? (Yes, No)	Yes
Is this domain intended to be Internet accessible? (Yes, No)	No
Is this domain intended to be accessible to the local network? (Yes, No)	Yes
Does this domain connect or bridge multiple networks? (Yes, No)	Yes

10.7 Exploitation Examples

The CERT/CC has received reports of vulnerabilities in network-enabled IV pumps, and other researchers have identified vulnerabilities in insulin pumps and pacemakers [Robertson 2013]. There have been no reports of exploitation in the wild.

11 Smart Sensors

11.1 Introduction

Smart sensors are one of the key technologies of ubiquitous computing, or the "Internet of Things" [Gubbi 2013]. Sensor technologies provide information about or control of a physical environment in response to certain stimuli. Two major types of sensors are being deployed by manufacturers: non-actuated and actuated sensors. Non-actuated sensors send information about the environment to a processing engine. Examples of non-actuated sensors include temperature sensors, vibration sensors, and soil moisture sensors. Actuated sensors send information about the environment but also receive commands or react to the environment in a particular way, usually by flipping an electronic switch or through mechanical manipulation. Examples of actuated sensors include wirelessly controllable smart lights, switches, and door locks. Both non-actuated and actuated sensors use wireless technologies to communicate. It should be noted that this domain is similar to SCADA, but it differs in that smart sensors use a greater number of standard network protocols and the Internet to facilitate communication. The differences between smart sensors and SCADA may decrease as SCADA gains more of the features that characterize this domain.

11.2 Recommendation

The CERT/CC recommends prioritizing this domain in 2014 and focusing more urgently on it in 2015 as the number and types of smart sensors increase. While only a few million of these active sensors are available, the continued consumer and commercial interest in these devices suggests that growth will be exponential [Gubbi 2013].

11.3 Time Frame

The market for this domain is estimated between $300B and $7.1T by 2020. In 2014, there will be 16 billion wireless connected devices, with estimates of 40 billion by 2020. CERT/CC recommends engaging the standard bodies and companies involved in smart sensor creation before the devices reach broad-scale adoption [Press 2014].

11.4 Impact

Smart sensors contain wireless communication technology, limited processing power, and sometimes an actuator or electronic switch that allows the sensor to react to the environment. These devices can be used in a variety of ways, from smart thermostats that use motion detection and machine learning to change the temperature in a house, to smart lights equipped with special sensors that can communicate via wireless mesh networks, ad hoc communication architectures that allow devices to communicate whenever they come in range, to any device. This range of capabilities suggests that adversaries will be able to conduct attacks that affect our environment in ways that are difficult to predict. Privacy can be compromised if embedded cameras in smart lights are exploited, or adversaries may use their access to smart thermostats to assess whether or not a person is home. As these sensors are integrated more fully into daily life and provide more control to the

user, it is likely that they will be increasingly considered a weak point into homes. Like many embedded devices with limited storage and processing, most of these sensors will likely be difficult to upgrade; this difficulty will likely lead to an increase in older, unpatched vulnerabilities.

11.5 Likelihood of Domain Success

The smart sensor domain is likely to be successful. Sales of the Nest smart thermostat and intelligent smoke alarm products have increased, reaching over one million sales per year and rising [Yarow 2014]. Smart lights are still nascent, but the massive energy savings are likely to make them ubiquitous in the commercial sector over the next several years [Digital Lumens 2013]. Belkin's consumer oriented WeMo line of smart plugs, lights, and devices provides remote control capability and some automation to everyday devices.

11.6 Exploitation Examples

In 2014, researchers found that the Belkin WeMo smart switch had several vulnerabilities that allowed an attacker to take complete control of the device, upload firmware, monitor other devices, and access the home network [Reuters 2014].

11.7 Triage Table

Table 10: Domain Triage for Smart Sensors

Characteristic/Question	Findings
Market Segment (Niche, Industry, Government, Consumer, Comprehensive, Other)	Comprehensive
Potential Market Segment Size (<$1B, $1B-$25B, $25B-$50B, >$50B)	>$50B
Projected Adopters (Percentage of market segment)	>75%
Current Market Penetration (Percentage)	<25%
Predicted Adoption Timeline (Years)	2 to 5 years
Does the technology have direct physical impact on the world? (Yes, No)	Yes
Can it cause direct property damage? (Yes, No)	Yes
Can it cause direct human harm? (Yes, No)	Yes
What is the scale of human harm? (none, single person, 1-10 people, > 10 people)	Single person
Digital consequence (Yes, No)	Yes
Is this domain intended to be remotely accessible? (Yes, No)	Yes
Is this domain intended to be Internet accessible? (Yes, No)	Yes
Is this domain intended to be accessible to the local network? (Yes, No)	Yes
Does this domain connect or bridge multiple networks? (Yes, No)	Yes

12 Vehicle Autonomy (Driverless Cars)

12.1 Introduction

Autonomous vehicles have the ability to move without direct commands from an operator. They can navigate to a destination using an autopilot-like capability, relying on onboard sensors including GPS, cameras, lasers, and radar for location. These onboard sensors also enable autonomous vehicles to avoid potential obstacles.

The development of autonomous vehicles is touted as a revolutionary capability that will increase the safety and reliability of vehicles [IIHS 2010, Simonite 2013]. Autonomous vehicles can also help optimize fuel economy and manage traffic congestion using vehicular communication systems.

In an effort to classify and evaluate autonomous vehicle capability, the National Highway Traffic Safety Administration (NHTSA) has established five levels to clarify the continuum of technologies [NHTSA 2013]:

- **Level 0 (No Automation)**: The driver is in complete and sole control of the vehicle (brake, steering, throttle, and motive power) at all times.
- **Level 1 (Function-Specific Automation)**: One or more vehicle controls are automated. Examples include electronic stability control or pre-charged brakes, where the vehicle automatically assists with braking to enable the driver to regain control of the vehicle or stop faster than possible by acting alone.
- **Level 2 (Combined-Function Automation)**: At least two primary control functions are automated and work in unison to relieve the driver of control of those functions. An example of combined-function automation is adaptive cruise control in combination with lane centering.
- **Level 3 (Limited Self-Driving Automation)**: All safety-critical functions are automated, and the driver can choose to enable those automated functions under certain traffic or environmental conditions. Vehicles at this level of automation monitor for changes in conditions that require transition back to driver control. The driver is expected to be available for occasional control but with sufficiently comfortable transition time. The Google Self-Driving Car is an example of limited self-driving automation.
- **Level 4 (Full Self-Driving Automation)**: The vehicle is designed to perform all safety-critical driving functions and monitor roadway conditions for an entire trip. Such a design relies on destination or navigation input from a human user, but a human driver is not expected to be available for control at any time during the trip. This type of vehicle can be occupied or unoccupied during a trip.

University research programs have studied various levels of automation over the years. These programs researched and demonstrated automation from basic research conducted in the 1980s and 1990s through the DARPA Grand Challenges in the mid-2000s. Autonomous vehicles recently developed by Google have logged hundreds of thousands miles in total on public roads without an

automation-related incident [Tannert 2014]. Commercial vendors such as Audi, Toyota, Nissan, and General Motors are currently investigating and demonstrating automation [Dassanayake 2014; Hsu 2013c; Turkus 2013; Krisher 2013].

12.2 Recommendation

The CERT/CC recommends prioritizing the autonomous vehicle domain for outreach and analysis in 2014. While the area is still nascent, it is being actively researched and tested by major manufacturers. Building an understanding and analysis capability of this field will allow for better outreach to manufacturers and researchers in the community. The massive safety benefits, transformation of lifestyle, and likely adoption mean that driverless cars will become an incredibly important technology. In addition, the potential for human harm and damage is very high, and the possible risks and vulnerabilities are not well understood.

12.3 Time Frame

Level 3 and 4 autonomous vehicles are not currently in production but are being tested by many major car manufacturers. Each type of vehicle offers various degrees of autonomy; adaptive cruise control, lane control, and coordinated behaviors between cars are among the capabilities being explored. Manufacturers in domains that do not have the same restrictions as on-road driving are exploring more advanced levels of autonomy. Systems in these areas may be marketed or described as mobile robotic systems; examples include automated material handlers (forklifts), parking lot shuttles, and mining vehicles [Seegrid 2013; Vaughn 2014; Caterpillar 2014].

Level 1 capabilities such as electronic stability control are being mandated for new models; many of these capabilities are available now or will be in the near term. Level 2 capabilities are about 5-10 years away. However, the building blocks for Level 2 capabilities are showing up in cars with Level 1 capabilities and in research and development projects such as the Super Cruise by General Motors [General Motors 2013]. At this time, Level 3 and 4 capabilities exist primarily in research environments and under strict human supervision.

12.4 Impact

Security concerns related to autonomous vehicles come predominantly from the potential for physical harm and damage. Digital disruption of autonomous vehicle systems has major implications for safety. For example, a software flaw affecting anti-lock brake systems in the Toyota Prius resulted in increased stopping distance [Toyota Motor Sales 2010].

Beyond the security concerns that are tied to basic flaws in implementation, there is the threat of active exploit. At DEFCON 2013, security researchers demonstrated attacks on vehicles [Greenberg 2013]. These attacks resulted in the compromise of the vehicle dashboard controls and displays, as well as the ability to cause a vehicle to brake or turn. Though these attacks were targeted at Level 1 and Level 0 capabilities, the implications for higher levels of autonomy are apparent. If low-level sensors and simplified systems are vulnerable to attack, compromise of Level 3 and 4 systems is inevitable.

12.5 Likelihood of Domain Success

Though fully autonomous vehicles are not ready for mainstream adoption, manufacturers are slowly rolling out functions that create the baseline of autonomous capability. In addition to technological challenges, policy and regulation are major barriers to large-scale deployment of autonomous vehicles. The automotive industry has many standards and regulations for vehicles. For broad adoption to occur, a consensus must be reached to ensure appropriate service levels for autonomy.

Individual states and legislative bodies are reviewing how autonomous vehicles can be governed by existing laws. States such as Florida, Nevada, and the District of Columbia have laws regarding the operation of autonomous vehicles but have differing opinions on liability and what constitutes an autonomous vehicle. The landscape of autonomous vehicles is so complex that the RAND Corporation created a guide to help inform policymakers about autonomous vehicles [Anderson 2014]. The report, *Autonomous Vehicle Technology: A Guide for Policymakers*, highlights the varying federal and state laws that may apply to vehicle autonomy as well as the liability issues surrounding autonomous vehicles.

12.6 Triage Table

Table 11: Domain Triage for Vehicle Autonomy

Characteristic/Question	Findings
Market Segment (Niche, Industry, Government, Consumer, Comprehensive, Other)	Comprehensive
Potential Market Segment Size (<$1B, $1B-$25B, $25B-$50B, >$50B)	>$50B
Projected Adopters (Percentage of market segment)	<25%
Current Market Penetration (Percentage)	<25%
Predicted Adoption Timeline (Years)	5 to 10 years
Does the technology have direct physical impact on the world? (Yes, No)	Yes
Can it cause direct property damage? (Yes, No)	Yes
Can it cause direct human harm? (Yes, No)	Yes
What is the scale of human harm? (none, single person, 1-10 people, > 10 people)	>10 people
Digital consequence (Yes, No)	Yes
Is this domain intended to be remotely accessible? (Yes, No)	Yes
Is this domain intended to be Internet accessible? (Yes, No)	Yes
Is this domain intended to be accessible to the local network? (Yes, No)	Yes
Does this domain connect or bridge multiple networks? (Yes, No)	Yes

12.7 Exploitation Examples

Researchers have identified information security problems in existing automotive systems that, for example, allow an attacker to modify the vehicle displays and readouts or send arbitrary commands on the controller area network (CAN) bus [Koscher 2010; Miller 2013]. Another area of concern is GPS spoofing, but mitigating factors such as GPS modernization may limit this threat [Humphreys 2008; Nighswander 2012]. So far, attacks have been limited, but they will likely increase in number, complexity, and damage as the technology becomes more connected.

13 Vehicular Communication Systems

13.1 Introduction

Vehicular communication systems combine wired and wireless technologies to enable intelligent transport systems for future cars, roads, and cities. Vehicular communication can be broken into two fields: Vehicle-to-Vehicle (V2V) communication and Vehicle-to-Infrastructure (V2I) communication. V2V provides vehicles with the ability to communicate their speed, position, and other status information to nearby vehicles. V2I allows for vehicles to receive and send information to smart roads, tollbooths, and other infrastructure components.

13.2 Recommendation

With millions of vehicles expected to use this technology—and the potentially fatal consequences of failure—this domain is of high priority for further vulnerability analysis. Because vehicle manufacturers and standards bodies typically have a long development period for creating standards and regulatory requirements, the CERT/CC recommends starting initial outreach and analysis efforts in 2014 to gain early influence in this domain.

13.3 Time Frame

The U.S. Department of Transportation (DoT) Intelligent Transport System Office has already field-tested 3,000 vehicles equipped with V2V in a 2012 pilot program. Both the DoT and the NHTSA are planning to support the advancement of this system in the consumer sector in 2014, and DoT officials have suggested that this technology may be mandatory for new vehicles starting in 2017 [NHTSA 2013; Nawaguna 2014].

13.4 Impact

The DoT and NHTSA have stated that, in the initial rollout of the technology in vehicles and infrastructure, V2V and V2I will only communicate safety warnings to the driver, not control functionality. The 5.9 Ghz spectrum is currently reserved by the Federal Communications Commission (FCC) for this technology, although it is shared with Wi-Fi devices. While the DoT and NHTSA insist that vehicular communication systems have many safeguards to protect privacy and automobiles, the simple act of providing an open communication path to a vehicle introduces risk. Recent vehicular automotive vulnerability research has demonstrated that the introduction of new technology into a vehicle can create behavior that the manufacturer did not intend [Miller 2013]. The future use of this technology as a control mechanism introduces even more risks, including those with fatal results.

13.5 Likelihood of Domain Success

This technology has a very high likelihood of coming to fruition. Manufacturers and regulators are working toward the development and deployment of this technology. Standards are available for use by manufacturers, pilot tests have been completed, and a mandate for use may be in place by 2017 [NHTSA 2013].

13.6 Triage Table

Table 12: Domain Triage for Vehicular Communication

Characteristic/Question	Findings
Market Segment (Niche, Industry, Government, Consumer, Comprehensive, Other)	Comprehensive
Potential Market Segment Size (<$1B, $1B-$25B, $25B-$50B, >$50B)	$1B-$25B
Projected Adopters (Percentage of market segment)	25-50%
Current Market Penetration (Percentage)	<25%
Predicted Adoption Timeline (Years)	5 to 10 years
Does the technology have direct physical impact on the world? (Yes, No)	Yes
Can it cause direct property damage? (Yes, No)	No
Can it cause direct human harm? (Yes, No)	No
What is the scale of human harm? (none, single person, 1-10 people, > 10 people)	None
Digital consequence (Yes, No)	Yes
Is this domain intended to be remotely accessible? (Yes, No)	Yes
Is this domain intended to be Internet accessible? (Yes, No)	No
Is this domain intended to be accessible to the local network? (Yes, No)	Yes
Does this domain connect or bridge multiple networks? (Yes, No)	Yes

13.7 Exploitation Examples

So far, there are no examples of exploitation of vehicular communication systems. Research in related domains has revealed systemic vulnerabilities that allow attackers to access the underlying electromechanics of the vehicle to gain control or provide improper readings to the driver [Checkoway 2011; Koscher 2010; Miller 2013]. In some cases the researchers were able to remotely compromise the vehicle.

14 Wearable Devices

14.1 Introduction

As devices become smaller and communications capabilities become cheaper, there is a strong interest in extending user interfaces onto devices that can be worn as watches, jewelry, fabrics, eyeglasses, and so on. The wearable devices domain focuses on the form and interfaces of these devices.

14.2 Recommendation

The CERT/CC does not recommend investing research in this area in 2014. While specific vulnerabilities will be introduced by specific products, the CERT/CC sees no novel threat vectors or changes to existing threat vectors that are not addressed by activities in other areas.

14.3 Time Frame

Wearable devices are rapidly increasing in popularity, with 90M wearable devices predicted to ship in 2014, and 164M in 2015 [Pai 2014]. The wearable space is currently very active with the rapid introduction of devices and supporting technologies. Google recently released a software development kit (SDK) for Android in support of wearables [Google 2014]. Such technologies significantly decrease the time to market for new devices.

14.4 Impact

Wearable devices have many interesting security implications. Malware targeted at a smartphone can easily be retargeted to a wearable device. An attacker could gain control of a device to, for example, control what a user sees in a pair of eyeglasses. However, the same scenarios exist for mainstream devices such as phones, heads-up-displays, and other portable computing equipment.

From a device perspective, most wearables are expected to connect primarily to smartphones for processing power and Internet connectivity. This domain may end up being similar to the smart sensor domain in terms of risks and capabilities.

14.5 Likelihood of Domain Success

It is difficult to tell which devices will succeed. Convenience, fashion, and miniaturization will likely continue to extend technology into every device. Specific additions to the Android platform and the Apple Watch indicate support for the wearable devices domain [Colon 2014, Padilla 2014].

14.6 Triage Table

Table 13: Domain Triage for Wearable Devices

Characteristic/Question	Findings
Market Segment (Niche, Industry, Government, Consumer, Comprehensive, Other)	Consumer
Potential Market Segment Size (<$1B, $1B-$25B, $25B-$50B, >$50B)	$1B-$25B
Projected Adopters (Percentage of market segment)	25-50%
Current Market Penetration (Percentage)	<25%
Predicted Adoption Timeline (Years)	5 to 10 years
Does the technology have direct physical impact on the world? (Yes, No)	No
Can it cause direct property damage? (Yes, No)	No
Can it cause direct human harm? (Yes, No)	No
What is the scale of human harm? (none, single person, 1-10 people, > 10 people)	None
Digital consequence (Yes, No)	Yes
Is this domain intended to be remotely accessible? (Yes, No)	Yes
Is this domain intended to be Internet accessible? (Yes, No)	No
Is this domain intended to be accessible to the local network? (Yes, No)	Yes
Does this domain connect or bridge multiple networks? (Yes, No)	Yes

14.7 Exploitation Examples

Google Glass has been hacked—mainly by users "jailbreaking" their own devices to add functionality—to provide access to the underlying device operating system [Freeman 2014].

15 Wireless Healthcare Asset Management

15.1 Introduction

Wireless healthcare asset management (WHAM) is the use of building-wide, geo-located wireless sensors that are attached to medical devices and equipment. The sensors report their location to a central server, allowing for a hospital to track all of its assets and, in some cases, report a device failure. The primary use of this technology is to improve the tracking and maintenance of assets, as lost or misplaced equipment is a recurring issue for many healthcare providers.

15.2 Recommendation

Due to the limited utility of the data stored by this technology, the lack of remote control of medical devices, and the rapid deployment by health care organizations, the CERT/CC does not recommend focusing on this technology in the near or far term.

15.3 Time Frame

Major manufacturers such as Cisco and GE are already selling sensors and asset tracking systems [Business Wire 2011, Cisco 2007]. Many hospitals have deployed or are considering deploying these systems because of the increased savings they provide.

15.4 Impact

The sensors used in WHAM are primarily passive sensors, meaning that they provide only the location information of physical objects to a server. The server tracks the location in the building and provides usage information related to the object (for example, names of staff who have used an intravenous pump). Most WHAM devices are not designed for two-way communication; a device simply provides notification of its current location. The lack of two-way communication and the low value of this information make any compromise of the main system a low-risk event to the victim [Ting 2011].

15.5 Likelihood of Domain Success

It is very likely that this technology will succeed. It is already deployed in many hospitals and other healthcare environments throughout the world.

15.6 Triage Table

Table 14: Domain Triage for Wireless Healthcare Asset Management

Characteristic/Question	Findings
Market Segment (Niche, Industry, Government, Consumer, Comprehensive, Other)	Consumer
Potential Market Segment Size (<$1B, $1B-$25B, $25B-$50B, >$50B)	$1B-$25B
Projected Adopters (Percentage of market segment)	>75%
Current Market Penetration (Percentage)	25-50%
Predicted Adoption Timeline (Years)	<2 years
Does the technology have direct physical impact on the world? (Yes, No)	No
Can it cause direct property damage? (Yes, No)	No
Can it cause direct human harm? (Yes, No)	No
What is the scale of human harm? (none, single person, 1-10 people, > 10 people)	None
Digital consequence (Yes, No)	Yes
Is this domain intended to be remotely accessible? (Yes, No)	Yes
Is this domain intended to be Internet accessible? (Yes, No)	No
Is this domain intended to be accessible to the local network? (Yes, No)	Yes
Does this domain connect or bridge multiple networks? (Yes, No)	Yes

15.7 Exploitation Examples

The CERT/CC is not aware of any exploitation attempts on this domain.

16 Conclusion

In preparing this report, the CERT/CC analyzed more than 1,700 emerging technologies identified by Gartner as emerging technologies through 2024. This analysis resulted in a list of 13 technology domains of cyber security interest. For each domain, a brief background, recommendation, time frame of adoption, impact of vulnerabilities, and exploitation example was developed. The recommendations provide a way to understand potential cyber security issues that may result as part of the domain's adoption in the future.

Appendix A: Underlying Technologies

Emerging technologies tend to leverage existing standards to improve the likelihood of adoption. By examining some of the underlying technologies and standards we can more accurately assess potential vulnerabilities. This section describes some of the general threats to these communication standards and gives short descriptions of the protocols evaluated as part of this report. This list is by no means comprehensive and is intended to provide coverage of popular protocols that exist today.

With the rapid development and deployment of devices, established infrastructure communication methods are quickly declining. New devices are relying more on wireless communication instead of using traditional wired communication. This departure from wired systems allows for rapid deployment and minimal infrastructure costs. As this shift continues, even within wireless communications there is movement from infrastructure wireless to mesh-based networking solutions. This focus on wireless communications in emerging technologies is the motivation behind this section and our emphasis on wireless communication technology and protocols.

One way to describe communication interconnects is by describing the network by spatial scope. Some common examples describing spatial scope are

- Body Area Network (BAN)
- Personal Area Network (PAN)
- Local Area Network (LAN)
- Wide Area Network (WAN)

Each of these networks has multiple options for communications protocols to use, from Bluetooth for BANs and PANs, to Ethernet (IEEE 802.3) for LANs, to WiMAX and LTE for WANs.

Another way to view these networks is by utilizing the common Open Systems Interconnection (OSI) model. This seven-layer model describes progressively higher level functions:

Table 15: Open Systems Interconnection Model

OSI Model	*Data unit*	*Layer*	*Function*
Host Layers	Data	7. Application	Network Process
		6. Presentation	Data representation
		5. Session	Interhost Communication
	Segments	4. Transport	Reliable delivery of packets
Media Layers	Packet/Datagram	3. Network	Addressing, routing, and delivery of datagrams
	Bit/Frame	2. Data link	Reliable, direct point-to-point data connections
	Bit	1. Physical	Direct point-to-point data connections

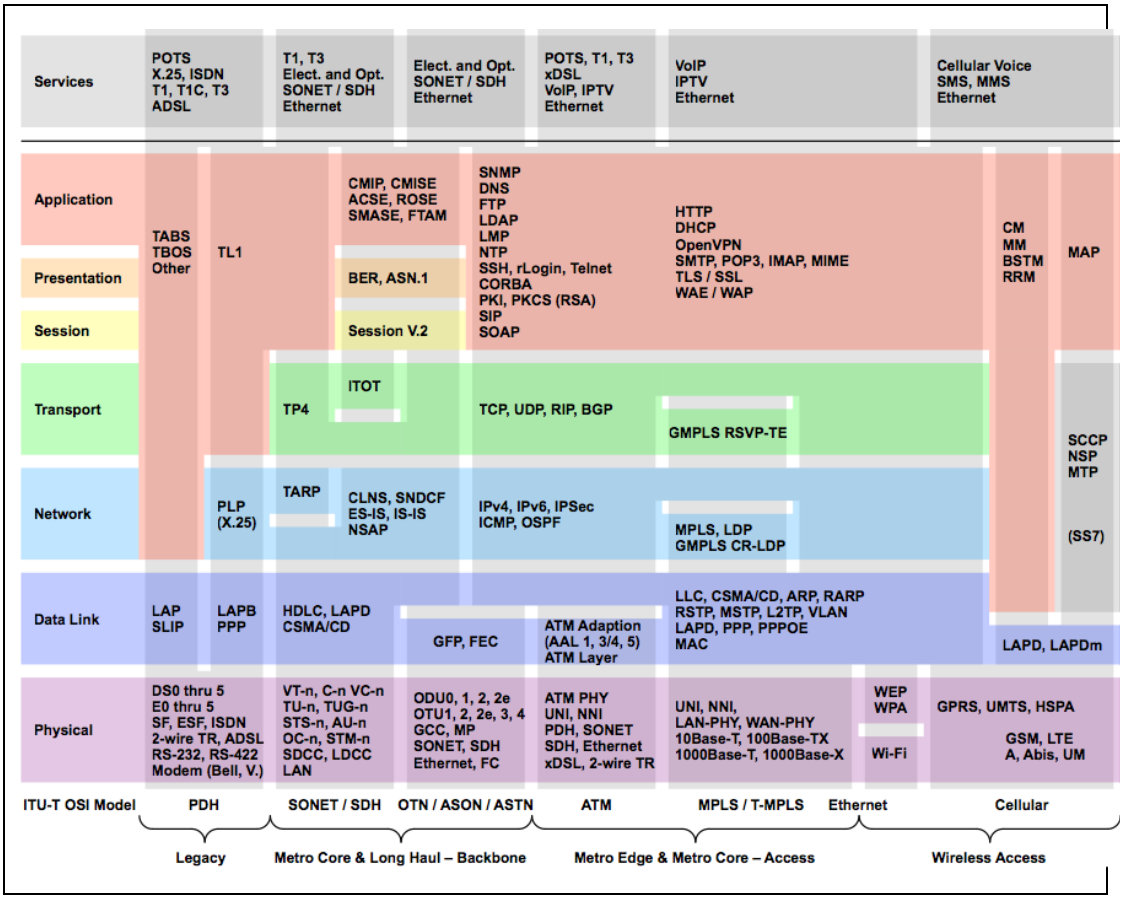

Figure 1: Communication Layers, Standards, and Technologies [Tele-Worx 2014]

As shown in Figure 1, protocols and implementations can exist at various layers and can even span layers. As wireless devices seek performance gains, new research has shown that blurring

the lines of the traditional OSI model is beneficial though others are pushing back for standardization [Raisinghani 2004; van der Schaar 2005; Mehlman 2014]. The varying scope and touch points for each of these protocols can be indicative of vulnerable locations. Well-defined boundaries are not necessarily in place, leaving good security boundaries left undefined. Each of these protocols could be vulnerable to security issues related to implementing the interface.

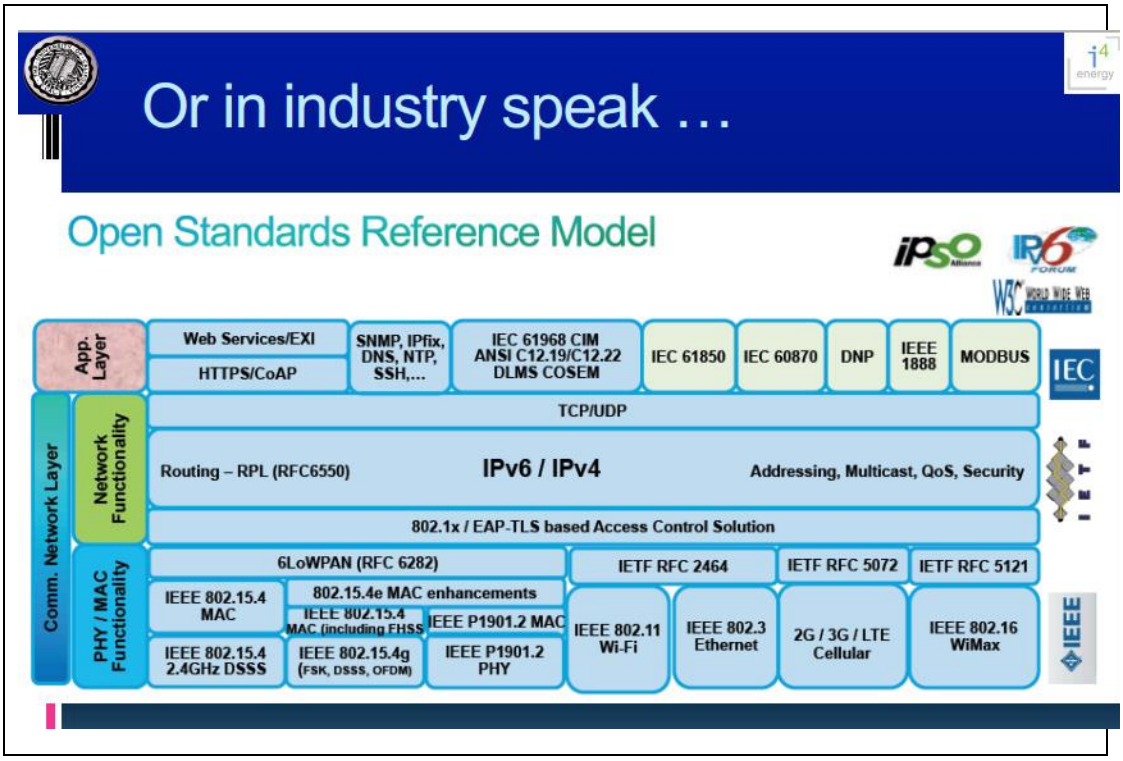

Figure 2: Open Standards Reference Model [Culler 2011]

Communication protocol stacks can have similar vulnerabilities given their position in the architecture. The lower layers are in direct communication with the hardware and can be vulnerable to different forms of hardware, firmware, and baseband attacks. In addition, high performance networks usually rely on direct memory access (DMA) to achieve high throughput. DMA has the potential for memory exploitation given the trust it has given the architecture. In addition to the underlying attacks, each protocol may have unique vulnerabilities (e.g., IEEE 802.11's WEP standard was broken, and Bluetooth has default pairing code vulnerabilities).

Table 16: Examples of Underlying Technologies

Protocol	Type of Network	Spatial Category	Typical Applications	Other Notes
6LoWPAN (IPv6 over Low power Wireless Personal Area Networks)	Point-to-Point, Point-to-Multipoint/Star	PAN		
ANT	Mesh, Point-to-Point, Tree, Point-to-Multipoint/Star	PAN	Primarily fitness performance monitoring	
Bluetooth (IEEE 802.15.1)	Point-to-Point, Point-to-Multipoint/Star (>v4.0)	PAN	Phones, Tablets, Media Players, Watches , Headsets, Speakers, Input Devices, etc.	
Bluetooth Low Energy	Point-to-Point	PAN	See Bluetooth.	Simpler, non-backwards-compatible version of Bluetooth.
Cellular	Point-to-Point	WAN	Phones, Computers, Tablets, Smart Meters, Cars	
Dash7 / ISO-IEC 18000-7	Point-to-Point	WAN	Sensor Networks	
Ethernet (IEEE 802.3)	Point-to-Point	LAN	Computers	
Global Positioning System	Broadcast-only	Worldwide	Position, Velocity, Time	
IEEE 802.15.4 (Low Rate Personal Wireless Network - LW-PWAN)	Point-to-Point	Depends on implementation	Sensor Networks	
NFC	Point-to-Point	NFC	Mobile Payments, low bandwidth communication	
RFID	Point-to-Point	PAN	Access control, Tracking solutions	
Wireless Access in Vehicular Environments (WAVE) (IEEE 802.11p)	Point-to-Point	CAN	Vehicle based communication networks.	
Wi-Fi___33 (IEEE 802.11)	Point-to-Point, Point-to-Multipoint/ Star	LAN	Phones, Computers	
ZigBee	Point-to-Point, Mesh	LAN	Sensor Networks	
Z-Wave	Point-to-Point, Mesh	LAN	Sensor Networks	

Appendix B: Domains and Supporting Technologies

	Z-Wave	Zigbee	WiFi	RFID	GPS	Ethernet	Cellular	Bluetooth	Bluetooth LE	802.11p	6LoWPAN
Autonomy			●	●	●		●	●		●	
Broadband-connected TVs			●			●					
Enterprise 3D Printing			●			●					
Home Area Network			●								●
Gesture Control								●	●		
Location Intelligence				●	●						
NFC				●							
Phone-as-Token Authentication			●				●				
Quantified Self				●	●			●	●		
Smart Appliances			●						●		
Smart Medical Devices			●			●		●	●		
Smart Sensors	●	●	●	●	●	●		●	●		●
Networked Telematics					●		●	●		●	
Vehicular Communication Systems										●	
Virtual Assistants			●				●				
Wearables			●					●	●		
Wireless Healthcare Asset Management				●	●						

References

URLs are valid as of the publication date of this document.

[ABI Research 2013]
ABI Research. *Wi-Fi to Play Dominant Role in the $25 Billion Smart Appliance Market.* https://www.abiresearch.com/press/wi-fi-to-play-dominant-role-in-the-25-billion-smar (October 30, 2013).

[Anderson 2014]
Anderson, James M.; Kalra, Nidhi; Stanley, Karlyn D.; Sorensen, Paul; Samaras, Constantine; & Oluwatola, Oluwatobi A. *Autonomous Vehicle Technology: A Guide for Policymakers.* http://www.rand.org/pubs/research_reports/RR443-1.html (2014).

[Burns 2014]
Burns, Matt. *The World's First Carbon Fiber 3D Printer Is Now Available to Order.* http://techcrunch.com/2014/02/18/the-worlds-first-carbon-fiber-3d-printer-is-now-available-to-order (February 18, 2014).

[Burns 2013]
Burns, Matt. *Enterprise-Class 3D Printers to Drop Under $2,000 by 2016, Says Report.* http://techcrunch.com/2013/03/29/enterprise-class-3d-printers-to-drop-under-2000-by-2016-says-report/ (March 29, 2013).

[Business Wire 2011]
Business Wire. *GE Healthcare and Cisco to Offer Hospitals a New Mobility Technology Platform for Improved Patient Flow and Asset Management.* http://www.business-wire.com/news/home/20110221005297/en/GE-Healthcare-Cisco-Offer-Hospitals-Mobility-Technology (February 21, 2011).

[Caterpillar 2014]
Caterpillar. *Caterpillar and Fortescue: Moving Forward with Commercial Installation of Autonomous Trucks*. https://mining.cat.com/cda/layout?m=112&x=7&id=4500932 (2014).

[Checkoway 2011]
Checkoway, Stephen; McCoy, Damon; Kantor, Brian; Anderson, Danny; Shacham, Hovav; & Savage, Stefan. *Comprehensive Experimental Analyses of Automotive Attack Surfaces.* http://www.autosec.org/pubs/cars-usenixsec2011.pdf (2011).

[Chen 2014]
Chen, Brian X. & Wingfield, Nick. *"Smart TVs" Are Next Bet for Makers as Sales Languish.* http://www.nytimes.com/2014/01/06/technology/smart-tvs-are-next-bet-for-makers-as-sales-languish.html (January 6, 2014).

[Cheng 2013]
Cheng, Roger. *AT&T, General Motors to Sell 4G LTE-Connected Cars Next Year.* http://www.cnet.com/news/at-t-general-motors-to-sell-4g-lte-connected-cars-next-year/ 2013 (February 24, 2013).

[Cisco 2007]
Cisco Systems. *The Cisco Location-Aware Healthcare Solution*. https://www.cisco.com/web/strategy/docs/healthcare/CLA_HealthcareSolution.pdf (June 2007).

[Colon 2014]
Colon, Alex. *Google to Release SDK for Android-Powered Wearables.* http://gigaom.com/2014/03/10/google-to-release-sdk-for-android-powered-wearables (March 10, 2014).

[Constantin 2014]
Constantin, Lucian. *Trojan Program Hijacks World of Warcraft Accounts Despite Two-Factor Authentication.* http://www.pcworld.com/article/2085280/trojan-program-hijacks-world-of-warcraft-accounts-despite-twofactor-authentication.html (January 7, 2014).

[Crosman 2013]
Crosman, Penny. *New Breed of Banking Malware Hijacks Text Messages.* http://www.americanbanker.com/issues/178_111/new-breed-of-banking-malware-hijacks-text-messages-1059745-1.html (June 10, 2013).

[Culler 2011]
Culler, David E. "The Internet of Every Thing – steps toward sustainability." Keynote, China Conference on Wireless Sensor Network. September 26, 2011. www.cs.berkeley.edu/~culler/talks/Culler-CWSN.pptx

[Danchev 2008]
Danchev, Danco. *Blizzard Introducing Two-Factor Authentication for WoW Gamers.* http://www.zdnet.com/blog/security/blizzard-introducing-two-factor-authentication-for-wow-gamers/1378 (July 2, 2008).

[Danova 2014]
Danova, Tony. *Just 3.3 Million Fitness Trackers were Sold in the US in the Past Year.* http://www.businessinsider.com/33-million-fitness-trackers-were-sold-in-the-us-in-the-past-year-2014-5 (May 5, 2014).

[Dassanayake 2014]
Dassanayake, Dion. *CES 2014: Audi Unveils Prototype Autonomous Car with "Auto-Pilot" System*. http://www.express.co.uk/news/science-technology/452562/CES-2014-Audi-unveils-prototype-autonomous-car-with-auto-pilot-system (January 7, 2014).

[Digital Lumens 2013]
Digital Lumens. *LightRules 2.5 Product Specifications*. http://www.digitallumens.si/images/LightRules_Specifications.pdf (2013).

[Dignan 2014]
Dignan, Larry. *3D Printing: Mainstream Adoption in 2014?* http://www.zdnet.com/3d-printing-mainstream-adoption-in-2014-7000024701 (January 2, 2014).

[Etherington 2014]
Etherington, Darrell. *Facebook Acquires Fitness and Activity Tracking App Moves*. http://techcrunch.com/2014/04/24/facebook-acquires-activity-tracking-app-moves/ (April 24, 2014).

[Fenn 2013]
Fenn, Jackie & Raskino, Mark. *Understanding Gartner's Hype Cycles*. http://www.gartner.com/document/code/251964 (July 2, 2013).

[Fink 2013]
Fink, Erica & Segal, Laurie. *Your TV Might Be Watching You*. http://money.cnn.com/2013/08/01/technology/security/tv-hack/ (August 1, 2013).

[Franco 2014]
Franco, Michael. *Skyforge, a Vending Machine for Your 3D-Printed Dreams.* http://news.cnet.com/8301-11386_3-57618264-76/skyforge-a-vending-machine-for-your-3d-printed-dreams (February 4, 2014).

[Freeman 2014]
Freeman, Jay. *Exploiting a Bug in Google's Glass*. http://www.saurik.com/id/16 (2014).

[George 2014]
George, Alexander. *New In-Car LTE Finally Brings Netflix Binges to Your Commute*. http://www.wired.com/2014/03/audi-cadillac-4g-lte/ (March 17, 2014).

[General Motors 2013]
General Motors. *"Super Cruise" Takes on Real-World Traffic Scenarios.* http://media.gm.com/media/us/en/gm/news.detail.html/content/Pages/news/us/en/2013/Apr/0429-cadillac-super-cruise.html (April 29, 2013).

[Google 2014]
Google. *Android Wear.* http://developer.android.com/wear/index.html (2014).

[Greenberg 2013]
Greenberg, Andy. *Hackers Reveal Nasty New Car Attacks—with Me Behind the Wheel*. http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/ (July 24, 2013).

[Greenberg 2012]
Greenberg, Andy. *Hacker Opens High Security Handcuffs with 3D-Printed and Laser-Cut Keys.* http://www.forbes.com/sites/andygreenberg/2012/07/16/hacker-opens-high-security-handcuffs-with-3d-printed-and-laser-cut-keys (July 16, 2012).

[Gubbi 2013]

Gubbi, Jayavardhana; Buyya, Rajkumar; Marusic, Slaven; & Palaniswami, Marimuthu. "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions." *Future Generation Computer Systems 29*, 7 (September 2013): 1645-1660.

[Hayashi 2013]

Hayashi, Kaoru. *Linux Worm Targeting Hidden Devices.* http://www.symantec.com/connect/blogs/linux-worm-targeting-hidden-devices (November 27, 2013).

[Hsu 2013a]

Hsu, Jeremy. *3-D Printed Gun's First Shot Has Big Implications.* http://spectrum.ieee.org/tech-talk/consumer-electronics/gadgets/3dprinted-guns-firing-shot-has-big-implications (May 8, 2013).

[Hsu 2013b]

Hsu, Jeremy. *First 3-D-Printed Metal Gun Shows Tech Maturity.* http://spectrum.ieee.org/tech-talk/robotics/industrial-robots/first-3dprinted-metal-gun-shows-tech-maturity (Nov 7, 2013).

[Hsu 2013c]

Hsu, Tiffany. *CES 2013: Lexus Driverless Car: "Technology Alone Is Not the Answer."* http://articles.latimes.com/2013/jan/07/autos/la-fi-tn-ces-hy-lexus-driverless-car-20130107 (January 7, 2013).

[Humphreys 2008]

Humphreys, Todd E.; Ledvina, Brent M.; Psiaki, Mark L.; O'Hanlon, Brady W.; & Kintner, Paul M. Jr. "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer," 2314-2325. *Proceedings of the 21st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2008)*. Savannah, Georgia, September 16-19, 2008. Institute of Navigation, 2008.

[IIHS 2010]

Insurance Institute for Highway Safety (IIHS). "New Estimates of Benefits of Crash Avoidance Features on Passenger Vehicles." *Status Report, 45*, 5 (May 20, 2010). http://www.iihs.org/iihs/sr/statusreport/article/45/5/2

[Koscher 2010]

Koscher, Karl et al. "Experimental Security Analysis of a Modern Automobile," 447-462. *IEEE Symposium on Security and Privacy*. Oakland, California, May 16-19, 2010. IEEE, 2010. http://www.autosec.org/pubs/cars-oakland2010.pdf

[Krisher 2013]

Krisher, Tom. *GM to Offer Nearly Self-Driving Car by 2020*. http://www.usatoday.com/story/money/cars/2013/08/30/gm-general-motors-self-driving-autonomous-car/2725091/ (August 30, 2013).

[Levy 2014]

Levy, Adam. *Can Google Unite a Fragmented Smart-TV Market?* http://www.fool.com/investing/general/2014/01/02/can-google-unite-a-fragmented-smart-tv-market.aspx (January 2, 2014).

[Leyden 2012]
Leyden, John. *Samsung's Smart TVs "Wide Open" to Exploits.* http://www.theregister.co.uk/2012/12/12/smart_tv_pwned (December 12, 2012).

[Mehlman 2014]
Mehlman, Jeffrey. *Cross-Layer Design: A Case for Standardization*. http://www.tc.ait.ac.th/faculty/teerapat/AT77.9019_Cross-Layer_Design_for_Wireless_Networks/Reading%20Assignments/Cross-layer%20Design_A_case_standardization.pdf

[Miller 2013]
Miller, Charlie & Valasek, Chris. *Adventures in Automotive Networks and Control Units*. http://illmatics.com/car_hacking.pdf (2013).

[Nawaguna 2014]
Nawaguna, Elvina. *Update 2-U.S. May Mandate "Talking" Cars by Early 2017*. http://www.reuters.com/article/2014/02/03/autos-technology-rules-idUSL2N0L814120140203 (February 3, 2014).

[NHTSA 2013]
National Highway Traffic Safety Administration (NHTSA). *U.S. Department of Transportation Releases Policy on Automated Vehicle Development*. http://www.nhtsa.gov/About+NHTSA/Press+Releases/U.S.+Department+of+Transportation+Releases+Policy+on+Automated+Vehicle+Development (May 30, 2013).

[Nielsen 2013]
The Nielsen Company. *Nielsen Estimates 115.6 Million TV Homes in the U.S., Up 1.2%.* http://www.nielsen.com/us/en/newswire/2013/nielsen-estimates-115-6-million-tv-homes-in-the-u-s---up-1-2-.html (May 7, 2013).

[Nighswander 2012]
Nighswander, Tyler et al. "GPS Software Attacks," 450-461. *Proceedings of the 2012 ACM Conference on Computer and Communications Security*. Raleigh, North Carolina, October 16-18, 2012. ACM, 2012.

[Padilla 2014]
Padilla, Richard. *Apple Reportedly Targeting Q3 2014 Launch for iWatch.* http://www.macrumors.com/2014/04/08/iwatch-launch-q3-2014/ (April 8, 2014).

[Pai 2014]
Pai, Aditi. *ABI: 90M Wearable Devices to Ship in 2014.* http://mobihealthnews.com/29532/abi-90m-wearable-devices-to-ship-in-2014/ (February 3, 2014).

[Press 2014]
Press, Gil. *Internet of Things By The Numbers: Market Estimates And Forecasts.* http://www.forbes.com/sites/gilpress/2014/08/22/internet-of-things-by-the-numbers-market-estimates-and-forecasts/ (August 22, 2014).

[Raisinghani 2004]
Raisinghani, Vijay T. & Iyer, Sridhar. "Cross-Layer Design Optimizations in Wireless Protocol Stacks." *Computer Communications 27*, 8 (May 2004): 720-724.

[Rao 2011]
Rao, Leena. *Sexual Activity Tracked by Fitbit Shows Up in Google Search Results.* http://techcrunch.com/2011/07/03/sexual-activity-tracked-by-fitbit-shows-up-in-google-search-results/ (July 3, 2011).

[Reuters 2014]
Reuters. *IOActive Lights Up Vulnerabilities for Over Half a Million Belkin WeMo Users.* http://www.reuters.com/article/2014/02/18/idUSnMKWhLTXta+1dc+MKW20140218 (February 18, 2014).

[RITA 2014]
Research and Innovative Technology Administration (RITA). *U.S. Department of Transportation Announces Decision to Move Forward with Vehicle-to-Vehicle Communication Technology for Light Vehicles*. http://www.its.dot.gov/press/2014/v2v_lightvehicles.htm (June 26, 2014).

[Robertson 2013]
Robertson, Jordan. *Medical Device Hackers Find Government Ally to Pressure Industry.* http://www.bloomberg.com/news/2013-07-22/medical-device-hackers-find-government-ally-to-pressure-industry.html (July 23, 2013).

[Rodriguez 2014]
Rodriguez, Salvador. *Refrigerator Among Devices Hacked in Internet of Things Cyber Attack*. http://articles.latimes.com/2014/jan/16/business/la-fi-tn-refrigerator-hacked-internet-of-things-cyber-attack-20140116 (January 16, 2014).

[Schomp 2014]
Schomp, Kyle et al. *Assessing DNS Vulnerability to Record Injection*. http://www.icir.org/mallman/pubs/SCRA14/SCRA14.pdf (2014).

[Seegrid 2013]
Seegrid Corporation. *Flexible Automated Guided Vehicles Anticipate Huge Growth in Europe 2014*. http://www.seegrid.com/press_release/seegrid_agv_growth_europe (December 24, 2013).

[Simonite 2013]
Simonite, Tom. *Data Shows Google's Robot Cars Are Smoother, Safer Drivers Than You or I.* http://www.technologyreview.com/news/520746/data-shows-googles-robot-cars-are-smoother-safer-drivers-than-you-or-i/ (October 25, 2013).

[Tannert 2014]
Tannert, Chuck. *Self-Driving Cars: Inside the Road Revolution*. http://www.fastcompany.com/3022489/innovation-agents/self-driving-cars-let-go-of-the-wheel (January 8, 2014).

[Tele-Worx 2014]
Tele-Worx. *Network Interface and Protocol Expertise–from the Application to the Physical Media*. http://www.med-worx.com/TELE-WORX/Interface_and_Protocol_Expertise.html (2014).

[Thomas 2014]
Thomas, Paul. *Despite the News, Your Refrigerator Is Not Yet Sending Spam*. http://www.symantec.com/connect/blogs/despite-news-your-refrigerator-not-yet-sending-spam (January 23, 2014).

[Ting 2011]
Ting, S. L. et al. "Critical Elements and Lessons Learnt from the Implementation of an RFID-Enabled Healthcare Management System in a Medical Organization." *Journal of Medical Systems 35*, 4 (2011): 657-669.

[Titlow 2013]
Titlow, John Paul. *How Hackers Can Infiltrate a 3-D Printer.* http://www.fastcolabs.com/3013165/inside-3-d-printings-weird-illicit-and-dangerous-fringe (August 6, 2013).

[Toyota Motor Sales 2010]
Toyota Motor Sales. *Toyota Announces Voluntary Recall on 2010 Model-Year Prius and 2010 Lexus HS 250h Vehicles to Update ABS Software.* http://pressroom.toyota.com/article_display.cfm?article_id=1868 2010 (February 8, 2010).

[Turkus 2013]
Turkus, Brandon. *Nissan Promising Autonomous Car Production by 2020*. http://www.autoblog.com/2013/08/27/nissan-promising-autonomous-car-production-by-2020/ (August 27, 2013).

[van der Schaar 2005]
van der Schaar, M. & Sai, Shankar N. "Cross-Layer Wireless Multimedia Transmission: Challenges, Principles, and New Paradigms." *Wireless Communications, IEEE 12*, 4 (August 2005): 50-58.

[Vaughn 2014]
Vaughn, Mark. *This Could Be Your First Autonomous Vehicle*. http://www.autoweek.com/article/20140109/carnews/140109862 (January 8, 2014).

[Wolff-Mann 2013]
Wolff-Mann, Ethan. *Cautious Bosch Says No Smart Appliances Just Yet.* http://refrigerators.reviewed.com/Features/Cautious-Bosch-Says-No-Smart-Appliances-Just-Yet.htm (January 7, 2013).

[Xiao 2013]
Xiao, Claud. *Security Attack to 3D Printing.* XCon2013 XFocus Security Conference. Beijing, China, August 22-23, 2013. http://www.claudxiao.net/Attack3DPrinting-Claud-en.pdf.

[Yarow 2014]
Yarow, Jay. *Nest, Google's New Thermostat Company, Is Generating A Stunning $300 Million in Annual Revenue*. http://www.businessinsider.com/nest-revenue-2014-1 (January 14, 2014).

[Zhong 2012]
Zhong, Han. *Primer: The Medical Device Industry.* http://americanactionforum.org/sites/default/files/OHC_MedDevIndPrimer.pdf (June 2012).

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	April 2015	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Emerging Technology Domains Risk Survey	FA8721-05-C-0003

6. AUTHOR(S)

Christopher King, Jonathan Chu, & Andrew Mellinger

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2015-TN-003

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFLCMC/PZE/Hanscom Enterprise Acquisition Division 20 Schilling Circle Building 1305 Hanscom AFB, MA 01731-2116	

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

In today's increasingly interconnected world, the information security community must be prepared to address emerging vulnerabilities that may arise from new technology domains. Understanding trends and emerging technologies can help information security professionals, leaders of organizations, and others interested in information security to anticipate and prepare for such vulnerabilities. This report, originally prepared in 2014 for the Department of Homeland Security United States Computer Emergency Readiness Team (US-CERT), provides a snapshot in time of the current understanding of future technologies. Each year, this report will be updated to include new estimates of adoption timelines, new technologies, and adjustments to the potential security impact of each domain. This report will also help US-CERT to make an informed decision about the best areas to focus resources for identifying new vulnerabilities, promoting good security practices, and increasing understanding of systemic vulnerability risk.

14. SUBJECT TERMS	15. NUMBER OF PAGES
emerging technology, vulnerabilities	60

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL